

CLERK'S OFFICE U.S. DISTRICT COURT
AT CHARLOTTESVILLE, VA
FILED

SEP 09 2024
BY: Laura A. Mostin CLERK
DEPUTY CLERK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

The undersigned Assistant United States
Attorney has reviewed and approves
the entire search warrant package.

Digitally signed by
Katie Medearis
Date: 2024.09.06
16:27:05 -04'00'
Katie Burroughs Medearis

IN THE MATTER OF THE SEARCH OF:
KINSEY COLLEEN STANSELL;
CELLULAR PHONE ASSOCIATED WITH
208-949-1504;
2633 HYDRAULIC ROAD,
CHARLOTTESVILLE, VIRGINIA 22901;
AND
2307 HYDRAULIC ROAD, UNIT 3069,
CHARLOTTESVILLE, VIRGINIA 22901

Case No. 3:24mj54

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR SEARCH WARRANTS**

I, Matthew S. Rader, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

A. Purpose of Affidavit

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure requesting issuance of warrants to search the following individual and locations:

- a. the person of **KINSEY COLLEEN STANSELL** (herein, "**STANSELL**");
- b. cellular phone associated with 208-949-1504 ("**TARGET CELLPHONE**");
- c. apartment residence located at 2633 Hydraulic Road, Charlottesville, Virginia 22901 ("**TARGET RESIDENCE**"); and
- d. storage unit 3069 located at 2307 Hydraulic Road, Charlottesville, Virginia 22901 ("**TARGET STORAGE UNIT**").

STANSELL is a resident of the **TARGET RESIDENCE**, the rental occupant of the **TARGET STORAGE UNIT**, and user of the **TARGET CELLPHONE**. **STANSELL**, the **TARGET CELLPHONE**, **TARGET RESIDENCE**, and the **TARGET STORAGE UNIT** are referred to

collectively as the “**TARGET SEARCH LOCATIONS**” and they are more fully described in Attachments A-1, A-2, A-3, and A-4 respectively, which are filed herewith and incorporated by reference herein. This affidavit is submitted to search the locations and individual described in Attachments A-1, A-2, A-3, and A-4 for the items detailed in Attachments B-1, B-2, B-3, and B-4.

2. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §§ 1001(a)(2) (false statements to government agents or agencies), 793(d) (communicating, delivering, or transmitting national defense information); 793(e) (gathering, transmitting, or retaining defense information), and 1924 (unauthorized removal or retention of classified documents or material) (collectively, the “Target Offenses”) have been committed by **STANSELL**, the user of the **TARGET CELLPHONE**, occupant of the **TARGET RESIDENCE**, and user of the **TARGET STORAGE UNIT**. As detailed below, there is also probable cause to believe evidence of the Target Offenses will be found at the **TARGET SEARCH LOCATIONS**.

B. Agent Background and Experience

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since November 2005. As part of my duties, I conduct national security investigations of various criminal violations, to include espionage, economic espionage, unauthorized removal and retention of national defense information, theft of intellectual property and trade secrets, and unauthorized access to/exceeding authorized access to computer systems, and other offenses. I have participated in the execution of numerous search warrants resulting in the seizure of classified and national defense information, computers, electronic media, digital storage devices and other physical and documentary evidence.

4. By virtue of my employment with the FBI, I have performed a variety of investigative techniques, including conducting arrests and executing federal search warrants. These search warrants have included the search and seizure physical and electronic evidence from residences, storage facilities, vehicles, and electronic devices used by United States Government employees, among others. I am also familiar with the fact that many criminals use their residences, storage facilities, vehicles, and electronic devices in connection with their illegal conduct including, but not limited to, storing and transporting evidence of their illegal activity. Relatedly, I have participated in national security-related investigations where evidence of the criminal conduct has been located in electronic devices, in hard copy format, and concealed from open view. I have also participated in interviews of witnesses, subjects, and targets in connection with investigating federal offenses. As a Special Agent, I am also an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

5. I am also an FBI certified polygraph examiner and have conducted polygraph examinations related to security screening, national security, and criminal investigations. In this role, I know that many applicants for United States government employment requiring a security clearance often omit or minimize derogatory information from their employment application and security screening paperwork. Those same omissions tend to be repeated in subsequent applications and clearance paperwork submissions for historical consistency and to avoid scrutiny.

C. Sources of Information

6. The facts in this affidavit are based on my personal knowledge and participation in the investigation, information gathered by other investigators, my review of United States Government (USG) reports, including information obtained from the United States Army (Army), open-source information, and other information that I believe to be reliable. Since this affidavit is

being submitted for the limited purpose of securing the requested search warrants, I have not included each and every fact known to me concerning this investigation. This affidavit also reflects my current understanding of facts relating to this investigation, but my understanding may change in the future as the investigation proceeds. Similarly, where information contained in reports and other documents or records are referenced herein, such information is also described in sum and substance and in relevant part only. This affidavit is intended to show only that there is sufficient probable cause for the requested warrants and does not set forth all my knowledge about this matter.

II. TARGET OFFENSES

7. Based on the information set forth below, I assert there is probable cause to conclude the Target Offenses have and/or are being committed by **STANSELL**, the user of the **TARGET CELLPHONE**, occupant of the **TARGET RESIDENCE**, and user of the **TARGET STORAGE UNIT**. The elements of the Target Offenses and related statutes are as follows:

8. Pursuant to 18 U.S.C. § 1001(a)(2), it is unlawful to knowingly and willfully make a materially false, fictitious, or fraudulent statement or representation to a department or agency of the United States.

9. Pursuant to 18 U.S.C. § 793(d), “[w]hoever, lawfully having possession of, access to, control over, or being entrusted with any document . . . or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and

fails to deliver it on demand to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

10. Pursuant to 18 U.S.C. § 793(e), "[w]hoever having unauthorized possession of, access to, or control over any document . . . relating to the national defense . . . willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

11. Pursuant to 18 U.S.C. § 1924, it is illegal for any officer, employee, contractor, or consultant of the United States, who, by virtue of his/her office, employment, position, or contract, becomes possessed of documents or materials containing classified information, to knowingly remove such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location.

12. Under Executive Order 13526, the unauthorized disclosure of material classified at the "TOP SECRET" ("TS") level, by definition, "reasonably could be expected to cause exceptionally grave damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(1), 75 Fed. Reg. 707, 707-08 (Jan. 5, 2010). The unauthorized disclosure of information classified at the "SECRET" ("S") level, by definition, "reasonably could be expected to cause serious damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(2). The unauthorized disclosure of information classified at the "CONFIDENTIAL" ("C") level, by definition, "reasonably could be expected to cause damage to the national security" of the United States. Exec. Order 13526 § 1.2(a)(3).

13. Sensitive Compartmented Information ("SCI") means classified information

concerning or derived from intelligence sources, methods, or analytical processes, which is further restricted, with the requirement that it be handled within formal access control systems established by the Director of National Intelligence.

14. Classified information of any designation may be shared only with persons determined by an appropriate United States Government official to be eligible for access, and who possess a "need to know." Among other requirements, for a person to obtain a security clearance allowing that person access to classified United States Government information, that person is required to and must agree to properly protect classified information by not disclosing such information to persons not entitled to receive it, by not unlawfully removing classified information from authorized storage facilities, and by not storing classified information in unauthorized locations. If a person is not eligible to receive classified information, classified information may not be disclosed to that person. In order for a foreign government to receive access to classified information, the originating United States agency must determine that such release is appropriate.

15. Pursuant to Executive Order 13526, classified information contained on automated information systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, or store classified information must be maintained in a manner that: (1) prevents access by unauthorized persons, and (2) ensures the integrity of the information.

16. 32 C.F.R. Parts 2001 and 2003 regulate the handling of classified information. Specifically, 32 C.F.R. § 2001.43, entitled "Storage," regulates the physical protection of classified information. This section prescribes that SECRET and TOP SECRET information "shall be stored in a GSA-approved security container, a vault built to Federal Standard (FHD

STD) 832, or an open storage area constructed in accordance with § 2001.53.” It also requires periodic inspection of the container and the use of an Intrusion Detection System, among other things.

III. PROBABLE CAUSE

A. Overview of the Investigation

1. *Background on STANSELL*

17. STANSELL has been employed at the National Ground Intelligence Center (NGIC), a component of the United States Army’s Intelligence and Security Command, in Charlottesville, Virginia since at least December 2023.¹ STANSELL serves as a civilian intelligence analyst and holds an active Top Secret security clearance.

18. Prior to working at NGIC, STANSELL served as an intelligence analyst while an active-duty member of the U.S. Army from approximately February 2020 through October 2023. During this timeframe, STANSELL served in multiple intelligence analyst roles in Italy and Germany, including an assignment to the Security Assistance Group – Ukraine (“SAG-U”).² In connection, STANSELL held a Top Secret security clearance and had access to classified intelligence related to various countries or regions, including, but not limited to, Russia, Ukraine, and Africa. STANSELL’s access included sensitive or classified materials found in digital and hard copy formats. Further, STANSELL continues to possess access to classified information in

¹ Among other responsibilities, NGIC provides general military intelligence on foreign ground forces, which may routinely include classified information.

² This information was gathered during investigative interviews conducted by Army Counterintelligence (ACI) and thereafter conveyed to the FBI.

her current assignment at NGIC.

B. STANSELL's Unauthorized Possession of Classified Materials and Related Admissions

19. In approximately November 2023, STANSELL was participating in a screening process, pursuant to a job application with another United States government agency. As detailed below, STANSELL made multiple admissions about her deliberate mishandling and retention of classified materials, inappropriate sharing or confirming of classified information with individuals without a need-to-know, and false statements related to her clearance forms.³

20. In particular, STANSELL admitted to possessing multiple classified documents at her current residence (i.e. the **PRIOR RESIDENCE**).⁴ She admitted retaining briefing aids, one map, and reports, which were classified either as SECRET or TOP SECRET (referred to collectively herein as the "Retained Classified Materials"). STANSELL stated the Retained Classified Materials were from her time in the Army.⁵ After admitting to retaining the classified materials, STANSELL confirmed she understood that someone would contact her to retrieve the classified documents and that she should not destroy the classified documents.

³ In general, "need-to-know" is a determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to, or knowledge, or possession of classified information in order to accomplish lawful authorized Government purpose. Prior to receiving a security clearance, individuals are typically briefed and advised of their obligations to safeguard information by their agency or employer. Thus, security holders are advised of the need-to-know concept and purpose of such informational safeguards.

⁴ The **PRIOR RESIDENCE** and **TARGET RESIDENCE** distinction is addressed in subsections herein.

⁵ Following her admissions, STANSELL's current employer confirmed to FBI that STANSELL did not return any of the Retained Classified Materials. Based on these circumstances and other information described herein, I believe STANSELL continues to possess the Retained Classified Materials and evidence of the Target Offenses at the **TARGET SEARCH LOCATIONS**.

21. The Army advised FBI that portions of STANSELL's work during her active-duty service related to the Russia-Ukraine conflict.

1. STANSELL's Transport of the Retained Classified Materials to Virginia.

22. During the applicant screening process, STANSELL described how she transported the Retained Classified Materials from Maine to her current residence in Virginia (i.e. the TARGET RESIDENCE) after her discharge from the Army. In particular, STANSELL explained she deliberately kept the map because she thought it would eventually be declassified and she wanted to show it to her family in the future.⁶

23. STANSELL initially denied showing anyone the Retained Classified Materials, but later acknowledged sharing classified information with M.D., a family member. She purported to store these items securely. However, STANSELL varied in describing the storage container used for the Retained Classified Materials: at one point, she described it as a locked safe, and at another, as a locking fireproof file cabinet. STANSELL also claimed to have transported the Retained Classified Materials in the locked container while moving to Virginia. STANSELL also stated these materials were stored in an unorganized bundle along with her personal papers.

2. STANSELL Practiced Classified Briefings in Her Unsecured Residence Overseas.

24. During her previously-described application process, STANSELL also admitted practicing classified briefings in her overseas residence with her family member, M.D., and not in

⁶ Declassification determinations are made by "original classification authorities" pursuant to E.O. 13526, which prescribes declassification dates of 10 or 25 years from the date of classification unless an original classification authority makes an earlier determination. *See* E.O. 12536 Sec. 1.5(a)-(b). Even the longer 25-year time horizons may be extended under certain circumstances. *See id.* Sec. 1.6(c).

a secure location. STANSELL stated M.D. possessed a clearance at the time she practiced her classified briefings with him at their shared residence. Based on my training and experience, I know that an individual's possession of a security clearance does not necessarily equate to a need-to-know. Further, I know that intelligence briefings routinely involve visual demonstratives, classified documents shared in whole or in part, and verbal representations of classified information. As part of FBI's investigation, I confirmed that M.D. possessed a security clearance at one time, but he did not serve in an intelligence-related capacity. Thus, M.D. likely did not have a need-to-know and his intentional receipt of the sensitive information through STANSELL's briefing rehearsals is consistent with a violation of one or more of the Target Offenses. Additionally, even if M.D. did have a need-to-know, STANSELL described practicing these briefings in their overseas private residence, which is not a secure area and, based on my training and experience, would not have been an appropriate designated location for the storage and/or discussion of classified material.

3. *STANSELL Admitted Discussing Classified Information with Uncleared Individuals and She Described Why the Contents of the Retained Materials Were Classified.*

25. During the application process described above, STANSELL also acknowledged discussing classified information with uncleared people (i.e., individuals without security clearances). STANSELL claimed to have done so, however, only if she assessed the information could be found in the news. Based on my training and experience, I know that confirming information shared via news outlets as a United States Government clearance holder can constitute unauthorized disclosure of classified information because it may inappropriately confirm the accuracy of information in the public sphere.

26. **STANSELL** also reported the briefing aids she possessed at her residence (i.e., the **TARGET RESIDENCE**) were hard copy aids allegedly constituting her own work product from when she was an analyst in the Army. **STANSELL** described the aids, including specifics of what she believed made them classified. In particular, and among other information, **STANSELL** stated the map contained both enemy and friendly troop locations. **STANSELL** acknowledged that the Retained Classified Materials may be designated TOP SECRET.

27. Based on my training and experience, I believe **STANSELL**'s awareness of the classification level of the materials, and her expressed desire to retain these materials due to their historical significance, is consistent with her deliberate commission of one or more of the Target Offenses. Her statements, and other information gathered during the course of the investigation, support a probable cause assessment that **STANSELL** likely continues to hold the Retained Classified Materials in her care, custody, or control at the **TARGET SEARCH LOCATIONS**. Here, **STANSELL** described her intention to retain the materials as well as her efforts to transport the Retained Classified Materials which is consistent with an ongoing desire to do so.

B. STANSELL's False Statements to the United States Government

28. In connection with two of her applications for United States government employment and related security clearance screening occurring between 2020 and 2023, **STANSELL** discussed drug use, which she failed to report on her Standard Form 86 ("SF-86").⁷

⁷ An SF-86 is a form used by the United States Government in conducting background investigations, re-investigations, and continuous evaluations of persons under consideration for or retention of national security positions, as defined in, 5 C.F.R. 732, and for individuals requiring eligibility for access to classified information under Executive Order 12968. The SF-86 form includes a warning section advising the individual completing the form that knowingly falsifying or concealing a material fact is a felony under 18 U.S.C. § 1001.

The SF-86 included the following question: "In the last seven years, have you illegally used any drugs or controlled substances?" The question further detailed that the "[u]se of a drug or a controlled substance includes injecting, snorting, inhaling, swallowing, experimenting with, or otherwise consuming any drug or controlled substance." STANSELL responded "no" to the above drug-use question.

29. During subsequent application screening in November 2023, STANSELL admitted her prior, undisclosed drug use occurred before and during her Army service *and* while she was an active United States Government clearance holder. For example, STANSELL stated she took double the amount of prescribed Adderall and combined it with nicotine and caffeine weekly from August 2021 until October 2023 for non-medical purposes while in the Army. STANSELL stated she crushed and snorted Adderall on approximately ten occasions. STANSELL further recounted multiple instances of unreported consumption of marijuana, mushrooms, "molly" (also known as 3,4-methylenedioxy-methamphetamine), acid, cocaine, and ketamine. During the interview, STANSELL acknowledged she deliberately omitted her past drug use from her security paperwork because she was worried about how it would look.

30. Based on my training and experience as a polygraph examiner and federal investigator, I know that individuals often minimize their misconduct to protect themselves or others. Through the course of this investigation, I identified a connection between STANSELL's family member, M.D., and an FBI narcotics investigation. This connection included at least 18 instances of bidirectional telephonic contact (calls and texts) in March 2023 between M.D. and J.M. J.M. was arrested on aggravated trafficking of illegal narcotics charges in April 2023. This connection is consistent with M.D., and potentially STANSELL, obtaining illegal controlled substances from the narcotics trafficker while STANSELL was a United States government

clearance holder. These telephone contacts and STANSELL's admissions about her drug use are also consistent with evidence of one or more of the Target Offenses being found on electronic devices located at the **TARGET SEARCH LOCATIONS**. Further, I know from training, experience, and common sense that narcotics are addictive substances and individuals often become dependent following extensive use. As a result, individuals will often continue to obtain, use, and abuse controlled substances even after admitting such misconduct to their employers.

C. **Probable Cause Evidence of the Target Offenses Will Be Found at the TARGET SEARCH LOCATIONS**

31. As detailed above, STANSELL moved to Charlottesville, Virginia in late 2023 to the **PRIOR RESIDENCE**.⁸ She admitted to transporting and keeping the Retained Classified Materials during her move. She also admitted to drug use as recently as October of 2023.

32. As recently as September 5, 2024, FBI physical surveillance and records checks confirmed STANSELL and M.D. reside at the **TARGET RESIDENCE**. FBI's investigation also revealed that STANSELL rents a storage unit (the **TARGET STORAGE UNIT**) in Charlottesville. Per subpoenaed records, STANSELL rented the **TARGET STORAGE UNIT** in approximately December of 2023. She is listed as the "occupant" on the agreement for the on-going month-to-month rental which was most recently paid in full through August 2024.

⁸ In approximately early September 2024, STANSELL moved to a different unit within the same apartment complex. Agents identified her new address based on three factors: 1) postal forwarding information provided to United States Postal Service; 2) physical surveillance tracking STANSELL traveling from her work and parking in front of the new residence; and (3) the same decorative wreath was moved from the prior residence door to the new residence door. For ease of reference STANSELL's residences are referred as the **PRIOR RESIDENCE** and **TARGET RESIDENCE**, respectively.

33. Of note, the **TARGET STORAGE UNIT** is located within walking distance of the **TARGET RESIDENCE**. **STANSELL** admitted to storing the Retained Classified Materials at the **PRIOR RESIDENCE** during her security processing in November 2023. **STANSELL's** rental of the **TARGET STORAGE UNIT** occurred *after* she indicated the Retained Classified Materials were located at her **PRIOR RESIDENCE**.

34. I know from training and experience that individuals will often store or transfer their belongings and personal effects between their residences when they move (i.e., **PRIOR RESIDENCE** to **TARGET RESIDENCE**) and to rented storage facilities. Personal effects may contain evidence of travel, work-related papers, drug paraphernalia, prescription records, photographs or videos documenting the acquisition and consumption of controlled substances, and communications with others about current affairs, work, drug use, and travel. Relatedly, I know individuals' personal effects often include previously-used electronic communication devices, such as old computers, cellphones, tablets, and sim cards. These electronic communication devices commonly contain information described above.

35. When discussing the Retained Classified Materials, **STANSELL** described varying storage mechanisms (i.e., a safe and a file cabinet) and a lack of organization (i.e., mixing classified materials within an unorganized bundle of personal papers). Based on **STANSELL's** own characterization of her handling of the Retained Classified Materials as being disorganized, and the fact she acquired the **TARGET STORAGE UNIT** *after* her admissions during her security processing, I submit it is probable that **STANSELL** wittingly or unwittingly transferred some or all of the Retained Classified Materials to the storage unit and/or other evidence of the Target Offenses will be found at the location. Further, **STANSELL** reported on her rental agreement forms that the **TARGET STORAGE UNIT** would contain "household items" and "furniture."

STANSELL previously indicated the Retained Classified Materials were stored within a filing cabinet or safe, which is consistent with a household item or furniture. On September 6, 2024, a representative from the company owning or operating the **TARGET STORAGE UNIT** confirmed to FBI that STANSELL still occupied the unit, and it was paid for through September 30, 2024.

36. Further, I know many government employees possess at least one, and often multiple, cellphones: namely, a personal device and a work device. I know that both work and personal cell phones often reveal information about a person's contacts, travel, work and personal activities, as well as conversations with others.

37. Here, FBI record checks and STANSELL's rental agreement both list her personal cellphone as bearing number 208-949-1504 (i.e., the **TARGET CELLPHONE**). Thus, I believe there is probable cause to conclude that one or more electronic devices will be in STANSELL's actual or constructive possession. The **TARGET RESIDENCE**, **TARGET STORAGE UNIT**, and STANSELL's employment location are in Charlottesville, which falls within the Western District of Virginia. Therefore, I believe there is probable cause to conclude STANSELL and the **TARGET CELLPHONE** will also be located within the District. Relatedly, I know that individuals will often transport their cellphone(s), personal belongings, work-related papers, and other items in their purse, backpack, briefcase, or simply on their person. Therefore, this affidavit is submitted in support of a warrant authorizing the search of STANSELL and personal effects under her control.

38. Based on my training and experience, I believe STANSELL's admissions provide probable cause that evidence of the Target Offenses will be found within the **TARGET SEARCH LOCATIONS**. These offenses including lying to the federal government about drug use, theft of

government property, conspiracy, as well as mishandling and unauthorized retention of classified materials.

D. Additional Probable Cause Related to Electronic Devices

39. I know from training and experience that individuals use electronic communications devices to send and receive messages, create and save documents, and take pictures or videos. Here, I believe that STANSELL likely communicated with others about events such as news involving the Ukraine-Russian conflict, her security screening process and any concerns arising after her inculpatory admissions, illegal drug acquisition and use, work overseas with the Army, relocation to Virginia, transfer of items to a storage unit, and/or her efforts to engage in, obfuscate, and/or conceal her involvement in the Target Offenses. Relatedly, I know that individuals seeking to conceal their involvement in the Target Offenses will often use encrypted messaging applications or take other steps to hide their activities from law enforcement and/or their employer.

TECHNICAL TERMS

40. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—

IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

IV. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

41. As described above and in Attachments B-1, B-2, B-3, and B-4, this application seeks permission to search for records and other evidence that might be found at the **TARGET SEARCH LOCATIONS**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

42. *Probable cause.* I submit that if a computer, electronic storage medium, or electronic device is found at the **TARGET SEARCH LOCATIONS**, there is probable cause to believe those records will be stored on the items, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

43. *Forensic evidence.* As further described in Attachments B-1, B-2, B-3, and B-4, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There

is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **TARGET SEARCH LOCATIONS** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution”

evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For

example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

44. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware

and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

45. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques including, but not limited to, computer-assisted scans of the entire medium that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

V. CONCLUSION


46. I submit that this affidavit supports probable cause for a warrant to search the **TARGET SEARCH LOCATIONS** described in Attachments A-1, A-2, A-3, and A-4 and seize the items described in Attachments B-1, B-2, B-3, and B-4.

VI. REQUEST FOR SEALING

It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrants. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the

targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,


Matthew S. Rader
Special Agent
Federal Bureau of Investigation

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me on this 9th day of September 2024, was placed under oath, and attested to the contents of this written affidavit.


JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE